US006963976B1

(12) **United States Patent**
Jutla

(10) **Patent No.: US 6,963,976 B1**
(45) **Date of Patent: Nov. 8, 2005**

(54) **SYMMETRIC KEY AUTHENTICATED ENCRYPTION SCHEMES**

(75) Inventor: **Charanjit Singh Jutla**, Elmsford, NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 752 days.

(21) Appl. No.: **09/705,998**

(22) Filed: **Nov. 3, 2000**

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/181**; 713/168; 707/9
(58) **Field of Search** 380/43, 10, 46, 380/37, 50, 4, 21, 216; 314/717; 713/165, 713/168, 181; 707/9

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,195,136 A * 3/1993 Hardy et al. 380/43
5,570,307 A * 10/1996 Takahashi 708/256
5,940,507 A * 8/1999 Cane et al. 713/165
5,974,144 A * 10/1999 Brandman 380/216

FOREIGN PATENT DOCUMENTS

EP 1063811 A1 * 12/2000 ..... H04L 9/06

OTHER PUBLICATIONS

M. Bellare, A. Desai, E. Jokiph, P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption: Analysis of DES Modes of Operation", 38th IEEE FOCS, 1997.

M. Bellare, J. Kilian, P. Rogaway, "The Security of Cipher Block Chaining", CRYPTO 94, LNCS 839, 1994.

V.D. Gligor, P. Donescu, "Integrity Aware PCBC Encryption Schemes", 7th Intl. Workshop on Security Protocols, Cambridge, LNCS, 1999.

V.G. Gligor, P. Donescu, Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes "http://www.nist.gov/aes/modes".

* cited by examiner

Primary Examiner—Charles Rones
Assistant Examiner—Jacob F. Bétit
(74) *Attorney, Agent, or Firm*—Louis P. Herzberg

(57) **ABSTRACT**

The present invention provides encryption schemes and apparatus which securely generate a cipher-text which in itself contains checks for assuring message integrity. It also provides compatible decryption schemes confirming message integrity. The encryption scheme generates a cipher-text with message integrity in a single pass with little additional computational cost, while retaining at least the same level of security as schemes based on a MAC. One embodiment encrypts a plain-text message by dividing the plain-text message into a multitude of plain-text blocks and encrypting the plain-text blocks to form a multitude of cipher-text blocks. A single pass technique is used in this process to embed a message integrity check in the cipher-text block. A message integrity check is embedded in the cipher-text blocks by embedding a set of pseudo random numbers, which may be dependent, but are pair-wise differentially uniform. We also describe an embodiment which is highly parallelizable.

47 Claims, 12 Drawing Sheets